AO-106 (Rev: 06/09)-Application for Search Warrant

FILED
MAR 21 2024
Mark C. McCartt, Clerk
U.S. DISTRICT COURT

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of *Usernames 'Brokenbnwowhiteboi,' 'Ohboyyyyy21,' and 'Knockershop' That are Stored at a Premises Controlled by MediaLab.ai, Inc..*

Case No. 24-MJ-184-JFJ

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A." This court has authority to issue this warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A).
located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252	Certain Activities Relating to Material Involving the Sexual Exploitation of Children

The application is based on these facts:

See Affidavit of SA Dustin Carder, HSI, attached hereto.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Dustin Carder, HSI
Printed name and title

Subscribed and sworn to by phone.

Date: 3/21/2024

Judge's signature

City and state: Tulsa, Oklahoma

Jodi F. Jayne, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

In the Matter of the Search of Information Associated with Kik Usernames 'Brokenbnwowhiteboi,' 'Ohboyyyyy21,' and 'Knockershop' That are Stored at a Premises Controlled by MediaLab.ai, Inc.	**Case No. _____**

Affidavit in Support of an Application for a Search Warrant

I, Dustin Carder, being duly sworn, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with Kik usernames **'Brokenbnwowhiteboi,' 'Ohboyyyyy21,'** and **'Knockershop'** that are stored at premises owned, maintained, controlled, or operated by MediaLab.ai, Inc., a holding company of consumer internet brands, offering messaging applications, online education platform, and various applications for users headquartered in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require MediaLab.ai, Inc. to disclose to the government records and other information in its possession, pertaining to the

individuals associated with **Kik usernames 'Brokenbnwowhiteboi,' 'Ohboyyyyy21,'** and **'Knockershop'** (hereinafter the "**SUBJECT ACCOUNTS**").

2. I have been employed as a Special Agent ("SA") with Homeland Security Investigations ("HSI") since December 2018. I am currently assigned to the Office of the Resident Agent in Charge in Tulsa, Oklahoma, and am currently assigned to investigate crimes involving child exploitation. While employed by HSI, I have investigated federal criminal violations related to child exploitation and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center's ("FLETC") twelve-week Criminal Investigator Training Program ("CITP") and the sixteen-week Homeland Security Investigations Special Agent Training ("HSISAT") program, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have received focused child exploitation training covering topics such as: interview techniques, live streaming investigations, undercover investigations, capturing digital evidence, transnational child sex offenders, and mobile messaging platforms utilized by these types of offenders. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252(a).

3. As part of my duties as a HSI Special Agent, I investigate criminal violations relating to child pornography, including the production, transportation, distribution,

receipt, and possession of child pornography, and the coercion/enticement of minors for sexual purposes, in violation of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422. I have been involved in several child pornography investigations and am familiar with the tactics used by individuals who coerce and entice minors, and collect and distribute child pornographic material.

4. The facts set forth in this affidavit are based on my personal observations and information provided to me by other law enforcement officers and individuals. Because I submit this affidavit for the limited purpose of showing probable cause, I have not included each fact that I have learned in this investigation. Rather, I have set forth only facts sufficient to establish probable cause to issue the requested warrant and I have not set forth all of my knowledge about this matter. Additionally, unless indicated otherwise, all statements and conversations described herein are related in substance and in part only, rather than verbatim.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 2252 (Certain Activities Relating to Material Involving the Sexual Exploitation of Children) have been committed by the individuals associated with the **SUBJECT ACCOUNTS**. There is also probable cause to search the information described in Attachment A for evidence of this crime and contraband or fruits of this crime as described in Attachment B.

Jurisdiction

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

Background of NCMEC and the CyberTipline Program

7. The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a private, non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further the mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and Child Victim Identification Program. NCMEC makes information submitted to the CyberTipline and Child Victim Identification Program available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers (ESPs), law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC performs its programs of work pursuant to its own private mission and independent business operations. NCMEC does not act in the capacity of or under the direction or control

of the government or law enforcement agencies. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.

8. NCMEC's CyberTipline is the nation's centralized reporting system for the online exploitation of children. The public and ESPs can make reports of suspected online enticement of children for sexual acts, child sexual molestation, child sex abuse material, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet. CyberTipline Reports (CyberTips) are distributed by NCMEC analysts to law enforcement agencies who may have legal jurisdiction in the place that victims and suspects are believed to be located based on information provided in the CyberTips..

Probable Cause

9. In October 2023, HSI Tulsa received information from the Tulsa County Sheriff's Office ("TCSO") regarding Bryon Alan LEE, a U.S. citizen and previously convicted sex offender. Multiple CyberTips from NCMEC had been generated regarding Google account "bryonalee1992@gmail.com" from Imgur, LLC[1],

[1] Imgur, LLC is an online content hosting site where users can view and share content such as images, GIFs, memes, videos, and reviews. Users can communicate with other users by posting public comments or sending private messages, GIFs, or emojis. Imgur is available on web browser and mobile application.

Dropbox, Inc.[2], and Discord[3] due to the uploading of numerous images of child pornography to their platforms. These leads span between August 2019 and August 2023. LEE is an enrolled member of the Cherokee Nation tribe and resides in Sapulpa, Oklahoma, within the territorial boundaries of the Muscogee Creek Nation, in the Northern District of Oklahoma.

10. On October 30, 2023, TCSO Detective Matt Gray was assigned four (4) CyberTips from NCMEC. The four CyberTips had email address "bryonalee1992@gmail.com" in common and spanned from 2019 to 2023. After an initial investigation, Gray determined that the suspect, Bryon LEE, was Native American and resided outside of his jurisdiction in Sapulpa, Oklahoma. Gray then sought my assistance in the investigation. The CyberTips will be detailed in the following paragraphs.

CyberTip 65655420

11. CyberTip 65655420 was reported by Imgur, LLC on March 9, 2020. Imgur reported that on August 7, 2019, a user with email address "bryonalee1992@gmail.com" uploaded 108 images to their platform that were flagged. Five IP addresses were associated with the uploads: two were Verizon Wireless, two were Cox Communications, and one was AT&T Wireless. The two

[2] Dropbox is a file hosting service operated by the American company Dropbox, Inc., headquartered in San Francisco, California, U.S. that offers cloud storage, file synchronization, personal cloud, and client software.

[3] Discord is an instant messaging and VoIP social platform. Users have the ability to communicate with voice calls, video calls, text messaging, media, and files in private chats or as part of communities called "servers."

Cox Communications IP addresses geolocated to Edmond, Oklahoma. It was later determined that LEE resided in Edmond, Oklahoma during this time.

12. I reviewed the images and observed them to consist of multiple prepubescent female victims topless, with bare chest exposed; multiple computer-generated media files depicting pornography; adult pornography; age-difficult females who are nude; and clothed prepubescent female victims posed in a provocative manner and/or wearing inappropriate clothing.

CyberTip 65654483

13. CyberTip 65654483 was reported by Imgur, LLC on March 9, 2020. Imgur reported that on November 25, 2019, a user with email address "bryonalee1992@gmail.com" uploaded 70 images to their platform that were flagged. The IP address used was 68.97.86.119, which geolocated to Edmond, Oklahoma, and was serviced by Cox Communications.

14. I viewed each image associated with the CyberTip. I observed many of the same images that were flagged in the previous CyberTip, which depicted prepubescent minor females posing in a provocative manner and/or wearing inappropriate clothing.

15. In April 2020, an Oklahoma State Bureau of Investigation (OSBI) analyst searched TLO[4] for email address "bryonalee1992@gmail.com." The email address was found to be linked to Bryon LEE, date of birth XX/XX/1992, at an apartment in Edmond, Oklahoma. Bryon LEE's name is fully listed in the suspect email address, as well as his birth year: 1992.

CyberTip 84142079

16. CyberTip 84142079 was reported by Dropbox on January 6, 2021. Dropbox reported that on January 5, 2021, at 01:10:42, a user with email address "bryonalee1992@gmail.com," username "Bryon Lee," with User ID number 3364911424, uploaded an image file to their platform that was flagged. The image with filename "Photo Jul 26, 11 00 58 PM.png" and MD5 value 40367f16f63a443c01823e845f1266b5 was categorized as "Apparent Child Pornography." This image was publicly available and was also viewed by one or more Dropbox employees. The image is described as a nude prepubescent white female with no breast development and no pubic hair. The minor victim (MV) appears to be under the age of 12. MV is bound by her hands and feet to a mirror using suction cups connected to binding straps. MV's vagina is visible in the image. This image meets the federal definition of child pornography, as stated in Title 18, United States Code, Section 2256.

[4] TransUnion's TLO is an online investigative database utilized by law enforcement containing personal information, including peoples' physical addresses, phone numbers, email addresses, and the contact details of possible relatives.

CyberTip 170916680

17. CyberTip 170916680 was reported by Discord on August 16, 2023. Discord reported that on August 16, 2023, at 00:58:32 UTC, username "dracusdemonica#0" with User ID number 246423663790915585 uploaded one image to their platform that was flagged. The image with filename "user23476379_f5a935dec2ec.jpg" with MD5 value fba226d428a8a43f456b5f733991bd05 was viewed by one or more Discord employees, was publicly available, and classified as "Apparent Child Pornography." The image is described as two minor female victims, one who is clothed, and the other who appears to be nude. The nude victim has little breast development. Both minor victims have their hands on the erect penis of an unknown male. The image meets the federal definition of child pornography, as stated in Title 18, United States Code, Section 2256.

18. Discord also provided verified phone number (918) 982-5823, and verified email address "bryonalee1992@gmail.com" that are associated with the account. The IP address utilized by the account during the upload was 98.178.189.190, which is serviced by Cox Communications and geolocates to Sapulpa, Oklahoma.

19. TCSO Detective Gray queried phone number (918) 982-5823 in Thomson Reuters' CLEAR[5]. Gray discovered the phone number was associated with Bryon

[5] CLEAR is a powerful research tool that assists law enforcement by combining billions of public records, to locate individuals, identify assets, and find key connections.

LEE at 710 West Teel Road in Sapulpa, Oklahoma. This falls within the Muscogee Creek Nation in the Northern District of Oklahoma.

Previous Sex Offense Involving Bryon Lee

20. In conducting this investigation, I learned that LEE is a registered sex offender for a 2020 Edmond Police Department case where LEE was convicted of Using Technology to Engage in Sexual Communication with a Minor (Oklahoma County CF-2021-1236). LEE received a 10-year suspended sentenced and was to be under the supervision of the Department of Corrections. This case involved LEE sending inappropriate and sexual communications and material via Facebook Messenger to a sixteen-year-old employee, his subordinate, at Taco Bell where he was the manager.

21. I learned that LEE is currently registered with the Muscogee Creek Nation Lighthorse Police (MCNLP). On October 31, 2023, I contacted the MCNLP and learned that his sex offender registration address is 710 West Teal Street, #24, Sapulpa, Oklahoma 74066. MCNLP advised that he registers every six months, and he last registered on July 18, 2023. MCNLP also had phone number (918) 982-5823 as his registered number, which is the same verified phone number connected to the Discord account described herein.

22. On November 3, 2023, HSI Tulsa electronically served Verizon Wireless with an administrative DHS summons for subscriber information for phone number (918) 982-5823 for a time frame of August 1, 2023, through the present.

23. On November 13, 2023, Verizon responded to the summons and provided the requested information. The number is registered to Bryon A. LEE with a contact address of 710 W. Teel Road, Trailer 24, Sapulpa, OK 74066. The account has been active since January 6, 2018. The email address associated with the Verizon account is bryonalee1992@gmail.com.

24. On November 15, 2023, I obtained federal search and seizure warrants in the Northern District of Oklahoma for the following: LEE's residence – 710 West Teel Road, Trailer 24, Sapulpa, OK 74066; LEE's vehicle – a red 2015 Chevrolet Spark with Oklahoma license plate CHN-562, VIN KL8CF6S91FC74; and LEE's person. The warrants were authorized by U.S. Magistrate Judge Jodi F. Jayne.

25. On November 16, 2023, at approximately 0755 hours, HSI special agents, task force officers, the Sapulpa Police Department, and the Muscogee Creek Nation Lighthorse Police served the search warrants at LEE's residence. Detective Matt Gray and I attempted to interview LEE in my vehicle. I showed LEE the search warrants, and explained what they were for. I advised LEE that he was not under arrest, but wanted to let him know what his rights were. LEE stated he did not want to speak without an attorney present. I then terminated the interview. As a result of the search warrants, multiple electronic devices, including LEE's cell phone, were seized at the scene, and later forensically examined.

Review of Dell Inspiron N5050 Laptop

26. I reviewed the data on a Dell Inspiron N5050 laptop computer (S/N: 823KJR1) seized during the search warrant. The owner of the device is listed as "Bryon," and the displayed computer name is "Bryon-PC." I located 26 files of child pornography on the device. Three are videos, and the remaining are images. There are five unique images of child pornography on the laptop; the remaining 18 are duplicates of those images.

27. One of the videos is twelve seconds long and depicts a prepubescent female victim in an outdoor setting. The victim's chest is exposed, and she has no visible breast development. There is a male masturbating with his penis positioned close to the victim's face. The male then ejaculates onto/into the face, hair, and mouth of the victim.

28. Another one of the videos is seven seconds long and depicts a prepubescent female victim wearing a purple shirt with a fairy or similar character on it. The female appears to be in the seated position. There is a male standing near the female with his penis exposed. The male appears to try and insert his penis into the victim's vagina. He then rubs his penis against her vagina. The victim is small in stature and had no visible pubic hair or development.

29. The remaining images and video depict prepubescent minor victims whose vaginas are displayed or are engaged in a sexual act.

Review of Samsung S21 FE Phone

30. I reviewed a Samsung S21 FE phone, IMEI: 350799511581772 seized during the search warrant. The Bluetooth name of this device is "Bryon's S21 FE." Multiple Chrome Autofill fields were also discovered for the name Bryon LEE, email address "bryonalee1992@gmail.com," and "DracusDemonica." I also located the usernames of "Oldddy4little," and "P3rvddy." I understand the first to mean that an older person is interested in a younger person, and the second is a short-hand form of "Perv" or "Pervert daddy." I was not able to determine which websites or programs the usernames were related to.

31. Based on images located, it also appears that LEE took pictures of his six-year-old daughter's buttocks and pubic/groin region while she slept. The victim is wearing underwear in both images. The time stamp associated with the files is September 15, 2023, at 3:20 AM. The victim's face was not shown in either image. In both images, the victim is laying on a black sheet with repetitive diamond or flower-shaped designs on it. Another image located shows LEE's daughter, fully clothed, with her face shown, standing next to the bed with the same sheet on it.

32. LEE's daughter, M.L. was later forensically interviewed and disclosed that LEE took pictures of her body, and videos of her butt when she had no clothes on. M.L. was given an outline of a body on a child so she could show what she meant by "butt;" M.L. circled the buttocks of the female child on the provided image.

33. I also located 41 files of child pornography on the device, with 28 of those being visually unique. Four of the files are videos, while the remaining are images. Two of the videos depict minor female victims who undress and display their vaginas on camera. One of the videos depicts a young female who takes off her clothing and masturbates on camera. Her vagina is visible. She has slight budding of the breasts. The remaining video depicts a school-aged adolescent female performing oral sex on an adolescent male while another adolescent male is engaging is vaginal or anal sex with her from behind. Most of the images depicts toddler-aged to approximately twelve-year-old female victims whose vaginas are displayed and/or are engaged in a sexual activity.

34. I located a partial Snapchat conversation between usernames "whiteboi2027512," and "randoma237722" while reviewing data on LEE's Samsung S21 phone. During this chat, an image of an 11-year-old female is shared, and the pair discuss the female in a sexually explicit manner. The below chat was located on LEE's phone.

Sender	**Recipient(s)**	**Message**	**Type**	**Message Date/Time - Central Time**
randoma237722	whiteboi2027512	Ye	Text	9/18/2023 8:42:39 PM
whiteboi2027512	randoma237722	I'd love to see her tiktok	Text	9/18/2023 8:44:28 PM
whiteboi2027512	randoma237722	Hey	Text	9/18/2023 8:39:45 PM
randoma237722	whiteboi2027512	Hi	Text	9/18/2023 8:39:49 PM

whiteboi2027512	randoma23722	Let's see her	Text	9/18/2023 8:40:06 PM
randoma23722	whiteboi2027512	She's 11	Text	9/18/2023 8:40:14 PM
whiteboi2027512	randoma23722	Ok	Text	9/18/2023 8:40:32 PM
randoma23722	whiteboi2027512	U wanna see	Text	9/18/2023 8:40:52 PM
randoma23722	whiteboi2027512		Call/Deleted message/Mini/ Game	9/18/2023 8:40:57 PM
whiteboi2027512	randoma23722	Yes	Text	9/18/2023 8:41:22 PM
whiteboi2027512	randoma23722	Cutie	Text	9/18/2023 8:41:58 PM
randoma23722	whiteboi2027512	Will u trib her	Text	9/18/2023 8:42:49 PM
whiteboi2027512	randoma23722	Yes! Anymore?	Text	9/18/2023 8:43:35 PM
randoma23722	whiteboi2027512	Only that one pic it was from her tiktok	Text	9/18/2023 8:44:10 PM
whiteboi2027512	randoma23722	She's got me so hard	Text	9/18/2023 8:44:11 PM
randoma23722	whiteboi2027512	Ik sameeee	Text	9/18/2023 8:44:23 PM

35. I was not able to view any media associated with this conversation. I know from previous child exploitation investigations that when "randoma23722" is asking "whiteboi2027512" if he will "trib" to the image that he means masturbate to the image. "Trib" is short for "tribute" or "tribute material." In most cases, this means that the person receiving the image or video will masturbate to it, and then send an image or video to the sender of themselves in or completing the act of masturbation.

36. I was able to determine that the "whiteboi2027512" account was native to LEE's Samsung S21 FE 5G, IMEI: 350799511581772. The "whiteboi2027512" username is similar to the current Kik username **'Brokenbnwowhiteboi.'**

New Device Seized

37. On February 29, 2024, an arrest warrant was issued based on a criminal complaint for LEE for the following offenses: 18 U.S.C. §§ 2251(d)(1)(A) & 2251(e) – Notice or Advertisement Seeking Child Pornography; 18 U.S.C. §§ 2252(a)(2) and (b)(1) – Receipt and Distribution of Child Pornography; and 18 U.S.C. §§ 1151, 1153, and 2252(a)(4)(A) and (b)(2) – Possession of Child Pornography in Indian Country. The arrest warrant was granted by U.S. Magistrate Judge Susan E. Huntsman in the Northern District of Oklahoma.

38. I sought the assistance of the U.S. Marshal's Northern Oklahoma Violent Crimes Task Force (USMS-NOVCTF) in placing LEE into custody. The USMS-NOVCTF arrested LEE without incident on February 29, 2024, at his employer, Five Guys restaurant, at 9635 Riverside Parkway, Tulsa, Oklahoma.

39. When LEE was taken into custody, he had personal property, including a Samsung Galaxy S21 FE 5G. This property was left at LEE's employer after he was arrested. Audrey Steinberg, LEE's girlfriend, was at a nearby retail store when the arrest happened. I notified Georgia Steinberg, Audrey Steinberg's mother, of the arrest so that she could assist Audrey in getting home, as Audrey does not drive.

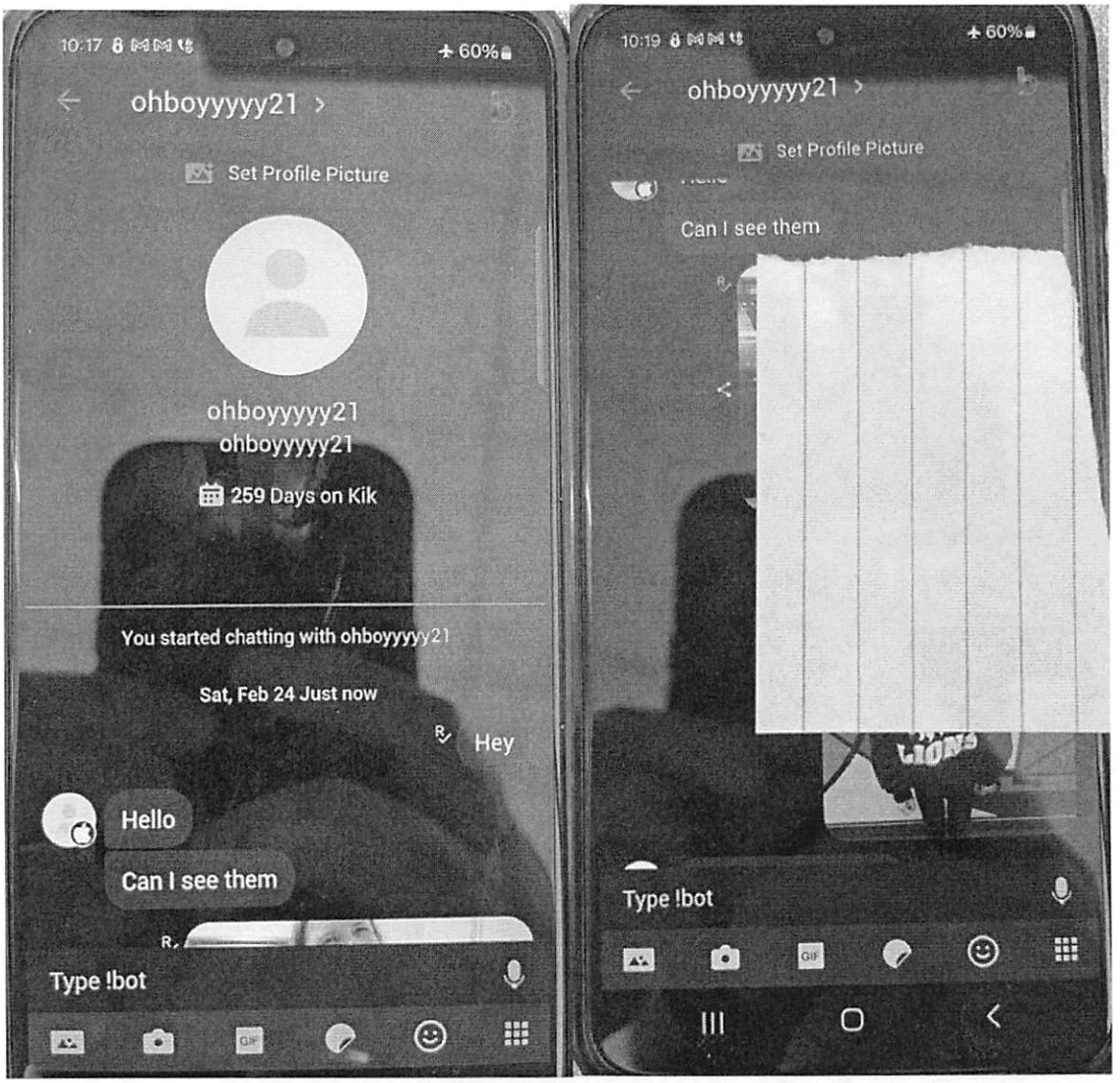
Georgia and Audrey retrieved LEE's personal property, including his phone, from LEE's employer.

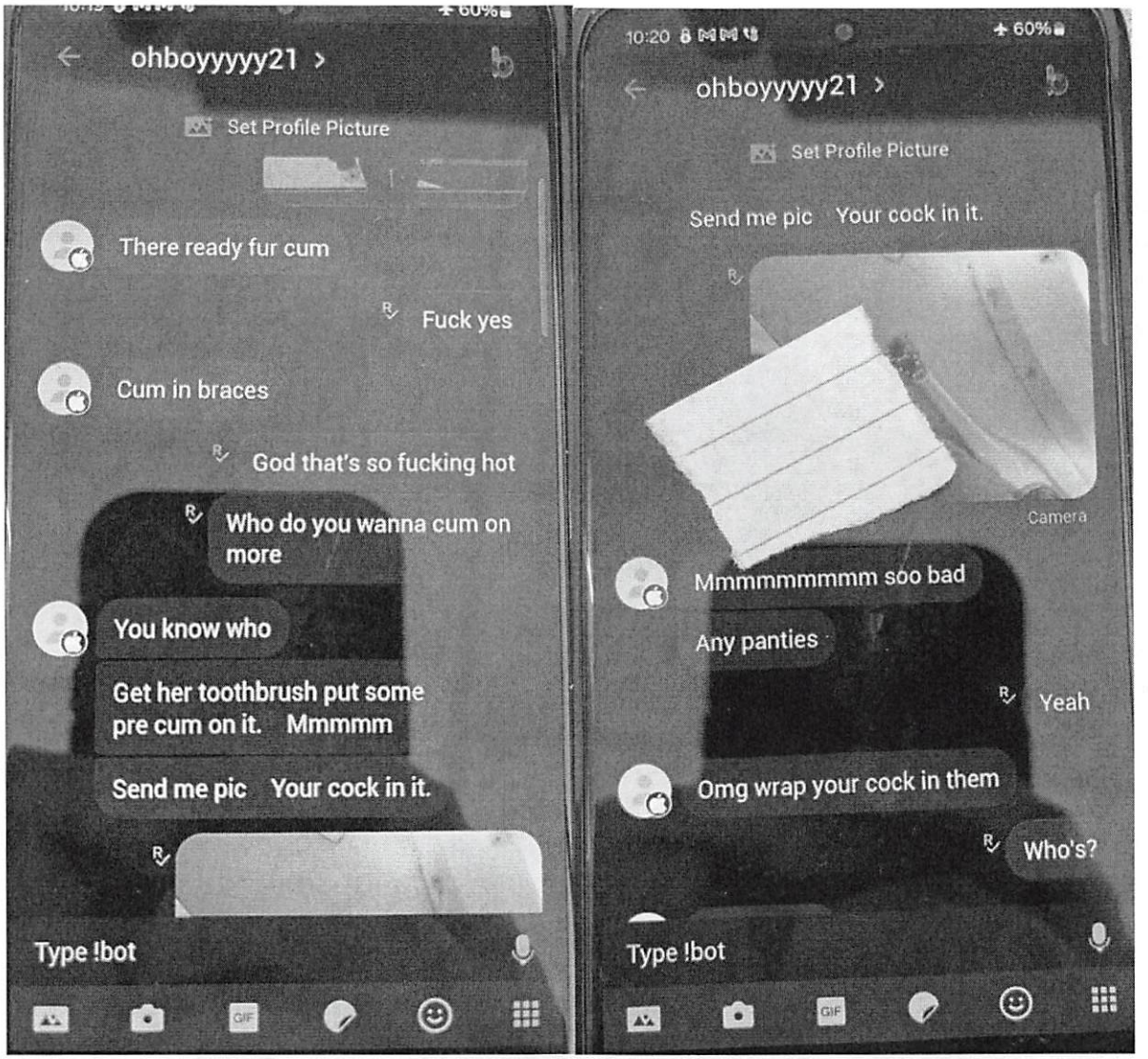
40. On March 5, 2024, Georgia Steinberg informed me that she had looked at LEE's phone and found pornography and records indicating LEE had been sending money to girls. Georgia stated that she did not see any nude images of children, although some of the images she was not able to tell the age of the person. I advised Georgia to stop looking at the device and that I would take custody of the phone and seek a search warrant to view the contents.

41. On March 6, 2024, HSI Task Force Officer (TFO) Don Stach and I met with Georgia and Audrey Steinberg at their residence in Tulsa. Georgia turned over the device to me. On March 14, 2024, a search warrant for this new device was granted by the Honorable Jodi F. Jayne, U.S. Magistrate Judge in the Northern District of Oklahoma.

42. After reviewing data on the device, I located multiple files of child pornography, including at least one image depicting the anal sodomy of an infant. Each of the flagged child pornography images were overlaid with text indicating that a user was selling child pornography and interested parties could contact him through various means listed to purchase the material. I also located numerous files of child exploitive and age-difficult material.

43. While manually reviewing the phone, I located two Kik conversations between usernames **'Brokenbnwowhiteboi'** and **'Ohboyyyyy21,'** and **'Brokenbnwowhiteboi'** and **'Knockershop.'** I was able to determine that username **'Brokenbnwowhiteboi'** was the username associated with LEE's device. The email address associated with this account is lewrachel747@gmail.com, which I also know to be associated with LEE through this investigation. These chats referenced children in a sexually explicit manner. I took pictures of the Kik chats on the device, and they are displayed below and on the following pages. I redacted a nude image of Audrey Steinberg and a clothed minor female, to protect her identity. In both chats outline below, LEE's statements are in the blue bubbles with white letters.


10:17
60%
ohboyyyyy21
Set Profile Picture
ohboyyyyy21
ohboyyyyy21
259 Days on Kik
You started chatting with ohboyyyyy21
Sat, Feb 24 Just now
Hey
Hello
Can I see them
Type !bot
10:19
60%
ohboyyyyy21
Set Profile Picture
Can I see them
Type !bot


ohboyyyyy21 >
Set Profile Picture
There ready fur cum
Fuck yes
Cum in braces
God that's so fucking hot
Who do you wanna cum on more
You know who
Get her toothbrush put some pre cum on it. Mmmmm
Send me pic Your cock in it.
Type !bot
10:20
60%
ohboyyyyy21 >
Set Profile Picture
Send me pic Your cock in it.
Camera
Mmmmmmmmm soo bad
Any panties
Yeah
Omg wrap your cock in them
Who's?
Type !bot

44. The minor female pictured in the chat was identified as LEE's 13-year-old sister. On March 19, 2024, I spoke with the LEE's father by phone. He confirmed that LEE has not had recent access to his sister. It appears that LEE may have used an older photograph of his sister in this chat, as she appears to have been between 7-9 years old in the image.

45. In this chat, LEE and the other subject discuss ejaculating on the minor female's braces and her toothbrush, and putting LEE's penis into the minor's underwear.

46. The second Kik chat located is similar in nature to the first. Photos are exchanged of a female and LEE and another subject discuss her age and LEE discusses wanting to cum on her face. See below for an excerpt of the chat::

LEE	I would love to see her
knockershop	(photo of a clothed young female sent)
LEE	Mmm level with me. How old is she?
knockershop	20s now 15 in the first ones 17 here
LEE	She's sexy
knockershop	(several images of the girl are sent) Glad you like her Tell me everything
LEE	I want to cum on her face in the first pic I love her smile and great tits

47. Based on these chats, it is probable that the **SUBJECT ACCOUNTS** contain evidence of the sexual exploitation of children.

48. In reviewing LEE's Kik account, I observed that the application on the device was 'Blue Kik.' I was unfamiliar with this version of Kik and conducted open-source research on it. According to www.medium.com, "Blue Kik is a modified version of Kik that "helps" improve the usability of the platform, but what most don't know is a lot of the reasons the platform is unusable is due to this mod. This mod provides users with exploitative ways to blackmail and harass users. This includes making your accounts unusable and being able to join Kik Live streams after being banned."

49. Kik, on their website, cites the dangers of third-party modified versions of Kik: "Kik takes the safety of our users very seriously. However, please understand that if you choose to download any modified, third-party versions of the Kik app, we cannot ensure your safety as a user. When you download a modified, third-party version of the Kik app (a.k.a. modded Kik) you are not only violating our Terms of Service but you may also be putting yourself, your privacy and your information at risk."

50. The dates requested for the search warrant are November 16, 2023, the day of the search warrant at LEE's residence when his original devices were seized, through February 29, 2024, the day of LEE's arrest.

Background on Kik and MediaLab.ai, Inc.

50. Kik is owned and operated by MediaLab.ai, Inc., a holding company of consumer internet brands, offering messaging applications, online education platform, and various applications for users headquartered in Santa Monica, California. Kik advertises itself as "the first smartphone messenger with a built-in browser." Kik Messenger allows users to "talk to your friends and browse and share any web site with your friends on Kik." According to their website, Kik Messenger, a free service easily downloaded from the Internet, has become the simplest, fastest, most life-like chat experience you can get on a smartphone. Unlike other messengers, Kik usernames - not phone numbers - are the basis for Kik user accounts, so Kik users are in complete control of with whom they communicate. In addition, Kik users can exchange images, videos, sketches, stickers and even more with mobile web pages.

51. The Kik app is available for download via the App Store for most iOS devices such as iPhones and iPads and is available on the Google PlayStore for Android devices. Kik can be used on multiple mobile devices, to include cellular phones and tablets.

52. In general, providers like Kik ask their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, and other identifiers such as an e-mail address. However, Kik does not verify that information. Kik also retains certain transactional information about the creation and use of each account on their systems, including the date on which the account was created, the length of service, records of

log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account.

53. Kik offers users the ability to create an identity within the app referred to as a "username." This username is unique to the account and cannot be changed. No one else can utilize the same username. A Kik user would have to create a new account in order to obtain a different username. The username for a particular Kik account holder is generally displayed in their Kik profile.

54. Given the ability for users to create multiple accounts that are not linked to a specific mobile device (i.e. a phone number), it has become a popular app used by people involved in the collection, receipt, and distribution of child pornography.

55. In my training and experience, an application user's IP log, stored electronic communications, and other data retained by the provider, can indicate who has used or controlled the application account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Kik account at a relevant time. Further, Kik account activity can show how and when the account was accessed or used. For example, as described herein, Kik logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the

chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Kik access, use, and events relating to the crime under investigation. Additionally, Kik account activity may provide relevant insight into the Kik account owner's state of mind as it relates to the offense under investigation. For example, information on the Kik account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

56. Therefore, the computers and systems of Kik, owned and operated by MediaLab.ai, Inc., are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Kik, such as account access information, transaction information, and other account information.

Characteristics Common to Individuals Who Exhibit a Sexual Interest in Children

57. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who exhibit a sexual interest in children, and who distribute, receive, possess, and/or access with intent to view child pornography:

i. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity;

ii. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;

iii. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years;

iv. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, on their person, to enable the individual to view the child pornography images, which are valued highly. Such individuals do not like to be away from their child pornography images for an extended period of time. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis;

v. Based on my training and experience and speaking with other special agents, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences;

vi. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos or other recordings, or engage in contact sex offenses with children. These images, videos or

other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child pornographic or child erotica images, videos or other recordings. Studies have shown there is a high cooccurrence between those who traffic in child pornography and commit sex offenses with children. Such individuals may also attempt to persuade, induce, entice, or coerce child victims in person or via communication devices to self-produce and send them child pornography or to meet in person for sex acts. These images, videos or other recordings are often collected, traded, or shared; and

vii. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

Information to be Searched and Things to be Seized

58. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require MediaLab.ai, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

Conclusion

59. Based upon the facts set forth in this affidavit, I believe that there is probable cause to believe that the location described in Attachment A contains evidence of violations of Title 18, United States Code, Section 2252 (Certain Activities Relating to Material Involving the Sexual Exploitation of Children), and Title 18, United States Code, Section 2422(b) (Coercion or Enticement of a Minor).

60. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on MediaLab.ai, Inc. Because the warrant will be served on MediaLab.ai, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully Submitted,

Dustin Carder
Special Agent
Homeland Security Investigations

Subscribed and sworn by phone on March 21, 2024

JODI F. JAYNE
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the account associated with Kik usernames **'Brokenbnwowhiteboi,' 'Ohboyyyyy21,'** and **'Knockershop'** (**SUBJECT ACCOUNTS**), that are stored at premises owned, maintained, controlled, or operated by MediaLab.ai, Inc., a company headquartered at 1222 6th Street, Santa Monica, CA 90401.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by MediaLab.ai, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of MediaLab.ai, Inc., regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to MediaLab.ai, Inc., or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), MediaLab.ai, Inc. is required to disclose the following information to the government for each account listed in Attachment A between November 16, 2023, through February 29, 2024:

(a) All contact and personal identifying information;

(b) All activity logs for the account and all other documents showing the user's posts and other Kik activities;

(c) All photos and videos uploaded by the SUBJECT ACCOUNTS and all photos and videos uploaded by any user that have that user tagged in them, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

(d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Kik usernames; groups and networks of which the

user is a member; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of MediaLab.ai, Inc.'s applications;

(e) All basic subscriber information,

(f) All call detail records,

(g) All detailed message logs,

(h) All content, including but not limited to message content,

(i) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that account, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

(j) All other records and contents of communications and messages made or received by the user, including all Messenger activity, messages, chat history, video and voice calling history, and pending "Friend" requests;

(k) All "check ins" and other location information;

(l) All IP logs, including all records of the IP addresses that logged into the account;

(m) All past and present lists of friends created by the account;

(n) All records of Kik searches performed by the account;

(o) The types of service utilized by the user;

(p) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(q) All privacy settings and other account settings, including privacy settings for individual Kik posts and activities, and all records showing which Kik users have been blocked by the account;

(r) All records pertaining to communications between MediaLab.ai, Inc. and any person regarding the user or the user's Kik account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 2252 for the **SUBJECT ACCOUNTS,** listed on Attachment A, including:

(a) Images of child pornography; files containing images and data of any type relating to the sexual exploitation of minors, and material related to the possession or production thereof, as defined in 18 U.S.C. § 2252;

(b) Information, correspondence, records, documents, or other materials pertaining to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors;

(c) Communications between the SUBJECT ACCOUNTS and others pertaining to the receipt, distribution, and/or possession of child pornography from November 16, 2023, through February 29, 2024;

(d) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

(e) Evidence indicating the account owner's state of mind as it relates to the crime under investigation; and

(f) The identity of the person(s) who created or used the SUBJECT ACCOUNTS, including records that help reveal the whereabouts of such person(s).